National Computer Board

Computer Emergency Response Team of Mauritius (CERT-MU)

Targeted Security Alert

Multiple Vulnerabilities in Microsoft Products

Original Issue Date: September 11, 2013

Severity Rating: High

Description:

Multiple vulnerabilities have been identified in Microsoft products and they can be exploited by remote attackers to gain knowledge of sensitive information, take full control of the affected systems, gain administrative rights, bypass security restrictions and cause a denial of service attacks. The vulnerabilities are as follows:

Vulnerability	Systems Affected	Description	Workarounds
Microsoft SharePoint Server vulnerabilities **CVE Info:** **CVE-2013-0081** **CVE-2013-1315** **CVE-2013-1330** **CVE-2013-3179** **CVE-2013-3180**	• Microsoft Office SharePoint Portal Server 2003 • Microsoft Office SharePoint Server 2007 • Microsoft Office Web Apps • Microsoft SharePoint Foundation 2010 • Microsoft SharePoint Server 2007 • Microsoft SharePoint Server 2010 • Microsoft SharePoint Server 2013 • Microsoft Windows SharePoint Services 2.x • Microsoft Windows SharePoint Services 3.x	Multiple vulnerabilities have been identified in Microsoft SharePoint, which can be exploited by malicious people to conduct cross-site scripting attacks, cause a Denial of Service and compromise a vulnerable system.	Users are advised to apply updates. More information about the updates is available on: http://technet.microsoft.com/en-us/security/bulletin/ms13-067
Vulnerability in Microsoft Outlook Could	• Microsoft Outlook 2007 • Microsoft Outlook 2010	The vulnerability could allow remote code execution if a user opens or previews a specially	Users are advised to apply updates. More information is

Allow Remote Code Execution **CVE Info:** **CVE-2013-3870**		crafted email message using an affected edition of Microsoft Outlook.	available on: https://technet.microsoft.com/en-us/security/bulletin/ms13-068
Multiple Vulnerabilities in Microsoft Internet Explorer **CVE Info:** **CVE-2013-3201** **CVE-2013-3202** **CVE-2013-3203** **CVE-2013-3204** **CVE-2013-3205** **CVE-2013-3206** **CVE-2013-3207** **CVE-2013-3208** **CVE-2013-3209** **CVE-2013-3845**	• Microsoft Internet Explorer versions 6,7,8,9 and 10	The most severe vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Internet Explorer. An attacker who successfully exploited the most severe of these vulnerabilities could gain the same user rights as the current user.	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/en-us/security/bulletin/ms13-069
Vulnerability in OLE Could Allow Remote Code Execution **CVE Info:** **CVE-2013-3863**	• Microsoft Windows XP • Microsoft Windows Server 2003	The vulnerability could allow remote code execution if a user opens a file that contains a specially crafted OLE object. An attacker who successfully exploited this vulnerability could gain the same user rights as the current user.	Users are advised to apply updates. More information is available on: https://technet.microsoft.com/en-us/security/bulletin/ms13-070
Vulnerability in Windows Theme File Could Allow Remote Code Execution **CVE Info:** **CVE-2013-0810**	• Microsoft Windows XP • Microsoft Windows Server 2003 • Microsoft Windows Vista • Microsoft Windows Server 2008	The vulnerability could allow remote code execution if a user applies a specially crafted Windows theme on their system. In all cases, a user cannot be forced to open the file or apply the theme; for an attack to be successful, a user must be convinced to do so.	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/en-us/security/bulletin/ms13-071

Vulnerabilities in Microsoft Office Could Allow Remote Code Execution **CVE Info:** **CVE-2013-3160**	• Microsoft Office 2003 • Microsoft Office 2007 • Microsoft Office 2010	These vulnerabilities could allow remote code execution if a specially crafted file is opened in an affected version of Microsoft Office software. An attacker who successfully exploited the vulnerabilities could gain the same user rights as the current user.	Users are advised to apply updates. More information is available on: http://technet.microsoft.com/en-us/security/bulletin/ms13-072
Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution **CVE Info:** **CVE-2013-1315** **CVE-2013-3158** **CVE-2013-3159**	• Microsoft Office 2003 • Microsoft Office 2007 • Microsoft Office 2010 • Microsoft Office 2013	These vulnerabilities could allow remote code execution if a user opens a specially crafted Office file with an affected version of Microsoft Excel or other affected Microsoft Office software. An attacker who successfully exploited the vulnerabilities could gain the same user rights as the current user.	Users are advised to apply updates. More information is available on: http://technet.microsoft.com/en-us/security/bulletin/ms13-073
Vulnerabilities in Microsoft Access Could Allow Remote Code Execution **CVE Info:** **CVE-2013-3155** **CVE-2013-3156** **CVE-2013-3157**	• Microsoft Office 2007 • Microsoft Office 2010 • Microsoft Office 2013	The vulnerabilities could allow remote code execution if a user opens a specially crafted access file with an affected version of Microsoft Access. An attacker who successfully exploited the vulnerabilities could gain the same user rights as the current user.	Users are advised to apply updates. More information is available on: http://technet.microsoft.com/en-us/security/bulletin/ms13-074
Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation of Privilege	• Microsoft Windows XP • Microsoft Windows Server 2003 • Microsoft Windows	The vulnerabilities could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application. An attacker must have valid logon credentials	Users are advised to apply updates. More information is available on: https://technet.microsoft.com/en-us/security/bulletin/ms13-076

CVE Info: **CVE-2013-3866**	Vista • Microsoft Windows Server 2008 • Microsoft Windows 7 • Microsoft Windows Server 2008 R2 • Microsoft Windows 8 • Microsoft Windows Server 2012 • Microsoft Windows RT	and be able to log on locally to exploit these vulnerabilities.	
Vulnerability in Windows Service Control Manager Could Allow Elevation of Privilege **CVE Info:** **CVE-2013-3862**	• Microsoft Windows 7 • Microsoft Windows Server 2008 R2	The vulnerability could allow elevation of privilege if an attacker convinces an authenticated user to execute a specially crafted application. To exploit this vulnerability, an attacker either must have valid logon credentials and be able to log on locally or must convince a user to run the attacker's specially crafted application.	Users are advised to apply updates. More information is available on: https://technet.microsoft.com/en-us/security/bulletin/ms13-077
Vulnerability in FrontPage Could Allow Information Disclosure **CVE Info:** **CVE-2013-3137**	• Microsoft FrontPage 2003 Service Pack 3	The vulnerability could allow information disclosure if a user opens a specially crafted FrontPage document. The vulnerability cannot be exploited automatically; for an attack to be successful a user must be convinced to open the specially crafted document.	Users are advised to apply updates. More information is available on: http://technet.microsoft.com/en-us/security/bulletin/ms13-078
Vulnerability in Active Directory Could Allow Denial of Service	• Microsoft Windows Vista • Microsoft Windows Server 2008	The vulnerability could allow denial of service if an attacker sends a specially crafted query to the Lightweight Directory Access Protocol (LDAP)	Users are advised to apply updates. More information is available on: https://technet.microsoft.com/en-

CVE Info: **CVE-2013-3868**	• Microsoft Windows 7 • Microsoft Windows Server 2008 R2 • Microsoft Windows 8 • Microsoft Windows Server 2012	service.	us/security/bulletin/ms13-079

Vendor Information

Microsoft

www.microsoft.com

References

Microsoft Security Bulletins

http://technet.microsoft.com/en-us/security/bulletin/ms13-sep

http://technet.microsoft.com/en-us/security/bulletin/ms13-067

https://technet.microsoft.com/en-us/security/bulletin/ms13-068

https://technet.microsoft.com/en-us/security/bulletin/ms13-069

https://technet.microsoft.com/en-us/security/bulletin/ms13-070

https://technet.microsoft.com/en-us/security/bulletin/ms13-071

http://technet.microsoft.com/en-us/security/bulletin/ms13-072

http://technet.microsoft.com/en-us/security/bulletin/ms13-073

http://technet.microsoft.com/en-us/security/bulletin/ms13-074

http://technet.microsoft.com/en-us/security/bulletin/ms13-075

https://technet.microsoft.com/en-us/security/bulletin/ms13-076

https://technet.microsoft.com/en-us/security/bulletin/ms13-077

http://technet.microsoft.com/en-us/security/bulletin/ms13-078

https://technet.microsoft.com/en-us/security/bulletin/ms13-079

Secunia

http://secunia.com/advisories/54741/

http://secunia.com/advisories/54737/

http://secunia.com/advisories/54735/

http://secunia.com/advisories/54750/

http://secunia.com/advisories/54742/

http://secunia.com/advisories/54725/

http://secunia.com/advisories/54739/

Please note that the members who do not want to receive the security alert, they can unsubscribe from CERT-MU mailing list by sending an e-mail to the following address: unsubscribe@cert-mu.gov.mu.

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378

Fax No: (+230) 208 0119

Gen. Info. : info@cert-mu.gov.mu

Incident: incident@cert-mu.gov.mu

Website: www.cert-mu.org.mu